Claims

1. (currently amended) A method for implementing an intrusion detection system in a network, comprising:

receiving a request from a central server at a software agent program to initiate intrusion detection services on a plurality of remote computers, wherein the request is issued by the central server in response to a notification of a network intrusion;

installing intrusion detection software on said remote computers via said software agent program; and

executing said intrusion detection software on said remote computers via said software agent program.

2. (currently amended) The method of claim 1 further comprising:

receiving from the central server a request to terminate intrusion detection services at said software agent program.

3. (original) The method of claim 2 further comprising:

monitoring for fulfillment of a stop condition.

4. (original) The method of claim 3 wherein said stop condition is based on network traffic conditions.

5. (currently amended) The method of claim 3 wherein said stop condition is an expiration time ~~of the request~~.

6. (cancelled)

7. (previously presented) The method of claim 1 further comprising the step of:

selecting said remote computers from a plurality of eligible computers.

8. (original) The method of claim 7 wherein said selecting step is accomplished based on a network map.

9. (original) The method of claim 7 wherein said selecting step is accomplished based on a knowledge base.

10. (original) The method of claim 1 wherein said request is verified using a cryptographic authentication scheme.

11. (original) The method of claim 1 wherein said request includes a stop condition indicating when to stop executing the intrusion detection software.

12. (currently amended) The method of claim 11 wherein said stop condition is an expiration time ~~of the request~~.

13. (original) The method of claim 11 wherein said stop condition is based on network traffic conditions.

14. (original) The method of claim 7 wherein said request is verified using a cryptographic authentication scheme.

15-22. (cancelled)

23. (currently amended) A system for detecting intrusions in a computer network comprising:

a plurality of computers executing software agents;

an intrusion detection server; and

a database configured to store at least one rule defining at least one response to a network intrusion, wherein said intrusion detection server is configured to send a request to install and execute intrusion detection software to software agents at a plurality of the computers when intrusion detection services are needed based on the at least one rule stored in said database.

24. (original) The system of claim 23 wherein said intrusion detection server increases the number of said plurality of computers executing intrusion detection software when a network intrusion is detected.

25. (original) The system of claim 23 wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software when the level of network traffic changes.

26. (original) The system of claim 23 wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software depending on the time of day.

27. (original) The system of claim 23 wherein said database contains information about the plurality of computers.

28. (original) The system of claim 27 wherein said information includes a map of said computer network.

29. (original) The system of claim 23 wherein said database contains a knowledge base.

30. (currently amended) An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to perform network intrusion detection, said steps comprising:

receiving notification of a network intrusion;

transmitting an installation request in response to the notification; and

installing intrusion detection software on a plurality of remote computers via a software agent program in response to the request.

31. (cancelled)

32. (previously presented) The article of manufacture of claim 30, further comprising the step of selecting said remote computers from a plurality of eligible computers.

33. (original) The article of manufacture of claim 32 wherein said selecting step is accomplished based on a network map.

34. (original) The article of manufacture of claim 32 wherein said selecting step is accomplished based on a knowledge base.

35. (original) The article of manufacture of claim 30 wherein said request is verified using a cryptographic authentication scheme.

36. (original) The article of manufacture of claim 30 wherein said request includes a stop condition indicating when to stop executing the intrusion detection software.

37. (original) The article of manufacture of claim 36 wherein said stop condition is an expiration time.

38. (original) The article of manufacture of claim 36 wherein said stop condition is based on network traffic conditions.

39. (new) The method of claim 1, wherein intrusion detection services are initiated at a plurality of remote computers selected based on a number of intrusion detection platforms that are currently active.

40. (new) The method of claim 1, wherein intrusion detection services are initiated at a plurality of remote computers selected based on predetermined numbers of maximum and minimum limits on a number of intrusion detection platforms.

41. (new) The method of claim 11, wherein the stop condition applies to all eligible computers.

42. (new) The method of claim 2, further comprising monitoring for fulfillment of a stop condition at each of the plurality of remote computers executing intrusion detection software.

43. (new) The method of claim 42, wherein the stop condition for each of the plurality of computers is based on a time during which each of the plurality of computers has been executing instruction detection software.